



POLÍTICA

“SEGURIDAD DE LA INFORMACIÓN PARA LA RELACIÓN CON PROVEEDORES”

Clasificación: Interna

Área: Procesos

Fecha de aprobación: SEPTIEMBRE - 2024

Fecha de actualización: SEPTIEMBRE - 2025

CONTENIDO

1.	OBJETIVOS	4
2.	ALCANCE	4
3.	DEFINICIONES.....	4
4.	RESPONSABILIDADES	5
5.	POLÍTICAS	6
5.1	CONSIDERACIONES GENERALES	6
5.2	CONSIDERACIONES ESPECIFICAS.....	6
5.3	CADENA DE SUMINISTRO DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN.....	7
5.4	SELECCIÓN DE PROVEEDORES DE BIENES Y/O SERVICIOS	7
5.5	CONTRATACIÓN DE PROVEEDORES DE BIENES Y/O SERVICIOS	8
5.6	ACCESO A LOS ACTIVOS DE INFORMACIÓN	8
5.7	IDENTIFICACIÓN DE RIESGOS DE RELACIONES CON TERCEROS	10
5.8	USUARIOS Y CONTRASEÑAS	12
5.9	GESTIÓN DE VULNERABILIDADES EN SERVIDORES Y/O APLICACIONES	12
5.10	REVISIÓN DE LA PROVISIÓN DE SERVICIOS.....	12
5.11	GESTIÓN DE CAMBIOS EN LOS SERVICIOS DE LOS PROVEEDORES	13
5.12	SEGURIDAD EN EL DESARROLLO DE SOFTWARE	13
5.13	TRANSFERENCIA DE INFORMACIÓN CON PROVEEDORES.....	14
5.14	RESPONSABILIDADES DE PROVEEDORES Y TERCERAS PARTES CON EL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.....	14
6.	DOCUMENTOS RELACIONADOS.....	14
7.	LISTA DE DISTRIBUCIÓN.....	15



AVISO DE PRIVACIDAD

“El presente documento es de uso interno. Su lectura está restringida a personal de la red de servicios REDFACILITO. La distribución o publicación de este documento sin previa autorización está completamente prohibida”



1. OBJETIVOS

Definir los requisitos para la protección de la confidencialidad, integridad y disponibilidad de la información de REDFACILITO a la cual los proveedores tienen acceso y mantener los niveles acordados para la entrega de servicios según acuerdos con proveedores.

2. ALCANCE

Esta política aplica para todos los proveedores que para la ejecución de su trabajo requieran acceder a la información, activos de información o infraestructura tecnológica de REDFACILITO, y aquellos que proporcionen productos o servicios que impactan al negocio.

3. DEFINICIONES

- **Activo:** Es todo lo que tiene valor para la organización y que por lo tanto requiere protección. (ISO/IEC 27005:2011, 8.2.2).
- **Acceso:** Puede ser lógico o físico, los cuales permiten que los usuarios puedan obtener información de la empresa. Lógico: ingreso mediante consola de administración a los activos de manera remota o local. Físico: ingreso a los edificios/oficinas técnicas, nodos, centros de datos.
- **Acuerdos de servicios con proveedores:** Son condiciones que el proveedor debe cumplir para brindar sus servicios, estos pueden estar establecidos en los contratos, términos de referencia o un documento de acuerdos de servicios.
- **Confidencialidad:** Propiedad de la información que pretende garantizar que esta solo es accedida por personas o sistemas autorizados.
- **Disponibilidad:** Propiedad de la información que pretende garantizar el acceso y uso de la información y los sistemas de tratamiento de esta por parte de los individuos, entidades o procesos autorizados cuando lo requieran.
- **Información:** Es un activo, que tal como otros importantes activos del negocio tiene valor para una empresa y requiere ser protegido adecuadamente. (ISO/IEC 27000:2018, 4.2.2)
- **Integridad:** Propiedad de la información que pretende mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.



- **Instalaciones de procesamiento de información:** Cualquier sistema de procesamiento de información, servicio o infraestructura, o la locación física que lo alberga. (ISO/IEC 27000:2018, 3.27).
- **Proveedor:** Persona o empresa que brinda o abastece de todo lo necesario para un fin a grandes grupos, asociaciones, comunidades, organizaciones.

4. RESPONSABILIDADES

Cargo/Rol	Responsabilidad
Gerencias y Jefaturas	<ul style="list-style-type: none"> • Identificar los proveedores que tienen acceso a los activos, información e instalaciones de procesamiento de información. • Gestionar los riesgos de seguridad de la información relacionados a los proveedores. • Asegurar que se implementen los controles de seguridad para atender los riesgos identificados. • Velar para que sus proveedores cumplan con esta política cuando accedan a los activos de REDFACILITO. • Revisar y monitorear el desempeño del proveedor sobre la seguridad de la información.
Oficial de Seguridad de la Información	<ul style="list-style-type: none"> • Definir, documentar y mantener actualizada la política de seguridad de la información para proveedores. • Distribuir y comunicar la política a las Gerencias/Jefaturas de REDFACILITO.
Asistente de Compras	<ul style="list-style-type: none"> • Asegurar que los proveedores catalogados como críticos cuenten con acuerdos de confidencialidad. • Comunicar esta política a los proveedores durante la suscripción de los contratos, o cuando surjan actualizaciones de la misma.



	POLÍTICA “SEGURIDAD DE LA INFORMACIÓN PARA LA RELACIÓN CON PROVEEDORES”	Código: PS-SGS-PO004
		Versión: 005
		Clasificación: Interna
		Página: 6 de 15

5. POLÍTICAS

5.1 Consideraciones generales

- a. El Coordinador de Infraestructura y Ciberseguridad en conjunto con los responsables de las áreas deberán identificar a los proveedores críticos, considerando aquellos que suministren productos o servicios esenciales para la operación de REDFACILITO o tenga acceso a la información y notificarlos al Asistente de Compras.
- b. Los requisitos de seguridad de la información deben acordarse con los proveedores críticos, para gestionar los riesgos asociados a los accesos de los activos de información.
- c. REDFACILITO podrá solicitar según aplique que los proveedores implementen redundancia en los activos críticos que tratan información y que tengan planes de respuesta ante eventos adversos que afectan la seguridad de dichos activos.

5.2 Consideraciones específicas

- a. Se debe establecer la autorización de los accesos a la información y el tipo de acceso de los proveedores.
- b. En base a la información que acceden los proveedores, se debe establecer requisitos mínimos de seguridad, como por ejemplo no divulgar la información, no almacenar la información en equipo que no estén autorizados, conectarse en forma segura, y otras similares.
- c. Se debe establecer acuerdos de confidencialidad y buen uso de la información que tengan acceso los proveedores.
- d. Se debe comprometer a los proveedores de gestionar los incidentes de seguridad en coordinación con REDFACILITO en los activos de información que son de su responsabilidad.
- e. El Asistente de Compras deberá compartir la presente política con los proveedores de REDFACILITO.
- f. El proveedor deberá coordinar con REDFACILITO cualquier cambio, transición o actualización de los activos de información, con la finalidad de evitar posibles incidentes que impacten al negocio.

- g. Se deberá revisar los accesos de los proveedores periódicamente, con la finalidad de identificar si no deben estar activos, o los privilegios no son los adecuados.
- h. Se deberá identificar si el proveedor trata información de carácter legal o normativo para establecer las medidas de seguridad adecuadas, por ejemplo, propiedad intelectual, datos personales y otros.
- i. Si REDFACILITO cree conveniente debe incluir en los acuerdos de servicio con los proveedores realizar auditorías específicas.

5.3 Cadena de suministro de tecnología de información y comunicación

- a. Se deberá identificar los servicios de tecnología que son administrados por el proveedor, el tipo de servicio y si los activos se encuentran en un sitio propio o en la nube.
- b. Solicitar que los proveedores exijan a sus colaboradores y proveedores que cumplan con los requisitos de seguridad establecidos de esta forma asegurar la seguridad de la cadena de suministro de tecnología de información.

5.4 Selección de proveedores de bienes y/o servicios

- a. En caso de requerir un servicio o producto de una entidad externa, la Gerencia General seleccionará al proveedor que cumpla con sus requerimientos y seguirá el proceso correspondiente para la adquisición, para su posterior implementación de acuerdo con las condiciones del contrato del producto o servicio adquirido en función a lo establecido en el documento **CN-GCN-PD002 - Gestión con proveedores.**
- a. El Asistente de Compras deberá notificar al Oficial de Seguridad de la Información cuando se encuentren en proceso de selección proveedores que tendrán acceso a la información de REDFACILITO. Esta notificación debe realizarse de manera oportuna, antes de la adjudicación del proveedor.
- b. El Asistente de Compras deberá incluir, dentro de las condiciones de participación en el proceso de concurso o selección, el documento **PS-SGS-FR008 - Evaluación de Cumplimiento y Seguridad de Proveedores Críticos.** Esta evaluación de cumplimiento y seguridad deberá ser completado por el proveedor como parte del proceso de selección.



- b. Los proveedores tendrán un plazo máximo para entregar la Evaluación de Cumplimiento y Seguridad de Proveedores Críticos, de acuerdo con los siguientes criterios:
- Proveedores con contratación urgente: 5 días calendario.
 - Otros proveedores: 10 días calendario.
- c. La evaluación completa, junto con cualquier evidencia que lo acompañe, deberá ser remitido al Oficial de Seguridad de la Información. Este último, en conjunto con el Coordinador de Infraestructura y Ciberseguridad–Lider de Base de Datos y Producción revisará las respuestas proporcionadas por el proveedor. Posteriormente, se emitirán recomendaciones de mejora, si aplica, en periodo máximo de 3 días que serán comunicadas al proveedor para su implementación antes de la contratación final.
- d. Anualmente se realizará una actualización/ revisión de los controles de seguridad implementado por los proveedores **PS-SGS-FR008 - Evaluación de Cumplimiento y Seguridad de Proveedores Críticos** y **PS-SGS-FR009 - Matriz de riesgos de seguridad de la información con proveedores.**

5.5 Contratación de proveedores de bienes y/o servicios

- e. El proveedor deberá firmar un acuerdo de confidencialidad, el cual se mantendrá posterior al término de la relación contractual por un periodo de al menos o mínimo cinco años.
- f. De acuerdo con el tipo de bien y/o servicio contratado, el proveedor deberá proporcionar el acuerdo de niveles de servicio y lista de escalabilidad para eventos o incidentes.
- g. El proveedor se obliga a dar a conocer y aplicar estas políticas en caso de subcontratar algún servicio relacionado con las actividades por las cuales fue contratado por REDFACILITO.

5.6 Acceso a los activos de información

- a. Los proveedores externos en caso de requerir el acceso para brindar soporte remoto o mejora del producto o servicio, el equipo de Infraestructura proporcionará este acceso mediante una sesión de escritorio virtual, de tal manera que se controle y monitoree la actividad del proveedor y debe ser registrado en el documento **TE-INF-FR015 - Control de acceso lógico a servidores.**



- b. El acceso remoto debe realizarse mediante protocolos seguros y filtrando el acceso por usuario y/o IP. El equipo utilizado por el proveedor durante el acceso temporal debe bloquearse mientras no se esté utilizando. Las sesiones inactivas se cerrarán luego de haber transcurrido el tiempo determinado por los administradores de la solución.
- c. El acceso físico por parte de los proveedores a los activos de información de REDFACILITO, deberá ser controlado y supervisado por el custodio o propietario del activo de información, el proveedor deberá respetar las normas establecidas por REDFACILITO para la ejecución de los trabajos en las instalaciones.
- d. Los proveedores deberán asegurar el cumplimiento del documento **PS-SGS-PO005 - Política de control de acceso.**
- e. El responsable del área a la que se relaciona el proveedor deberá identificar los permisos y aplicativos específicos a los que el proveedor deberá tener acceso, esta identificación debe ser realizada de acuerdo con las necesidades del proyecto o servicio y considerando los principios de mínimo privilegio y una vez identificados los permisos y aplicativos, el responsable del área deberá notificar al Coordinador de Infraestructura y Ciberseguridad.
- f. La notificación deberá incluir una descripción clara de los permisos requeridos, los aplicativos a los que se accederá, y la justificación de la necesidad de dichos accesos.
- g. El Coordinador de Infraestructura y Ciberseguridad, deberá registrar los aplicativos y permisos a los que el proveedor tendrá acceso en el documento **TE-SYC-FR016 - Matriz de roles y accesos a aplicaciones - Internos.**
- h. El responsable de área deberá enviar el formulario **TE-SYC-FR001 - Solicitud de usuarios** al equipo de Seguridad y Control, la solicitud debe incluir la fecha en la que los accesos deben ser deshabilitados, asegurando que no existan accesos abiertos innecesariamente.
- i. El equipo de Seguridad y Control deberá asegurarse de que los accesos se deshabiliten en la fecha indicada en la solicitud.
- j. Cualquier cambio en la estructura de roles y accesos deberá ser notificado inmediatamente al Coordinador de Infraestructura y Ciberseguridad.



5.7 Identificación de riesgos de relaciones con terceros

- a. Los riesgos de seguridad relacionados con proveedores de servicios y terceros que tengan acceso a la información de REDFACILITO, deberán de ser identificados y considerados durante el proceso de evaluación de riesgos en el documento **PS-SGS-FR009 - Matriz de riesgos de seguridad de la información con proveedores.**
- b. Se deberá considerar la siguiente fórmula para calcular el nivel de riesgos para los proveedores:

Nivel de riesgos = Probabilidad * Impacto

Nivel de Probabilidad	Valor	Definición
Alta	3	Es muy probable que el riesgo ocurra en un futuro cercano, basado en la frecuencia o historial de eventos similares.
Media	2	El riesgo tiene una probabilidad moderada de ocurrir. Es posible que ocurra, pero no es algo que se espera con regularidad.
Baja	1	El riesgo es poco probable que ocurra, ya que las condiciones que lo favorecen rara vez se presentan.

Nivel de Impacto	Valor	Definición
Alta	3	El impacto en la organización sería muy significativo, con consecuencias graves como pérdida financiera considerable, daño reputacional o incumplimiento regulatorio.
Media	2	El impacto sería moderado, causando problemas operacionales, costos adicionales o menores problemas legales o reputacionales.



Nivel de Impacto	Valor	Definición
Baja	1	El impacto sería leve, con consecuencias mínimas que no afectarían de manera significativa las operaciones o la estabilidad de la organización.

		IMPACTO			
		Bajo	Medio	Alto	
PROBABILIDAD	Bajo	1	Bajo (1)	Bajo (2)	Medio (3)
	Medio	2	Bajo (2)	Medio (4)	Crítico (6)
	Alto	3	Medio (3)	Crítico (6)	Crítico (9)

- c. **Notificación de evaluación de seguridad:** Cada vez que un proveedor sea incorporado y aplique **PS-SGS-FR008 - Evaluación de Cumplimiento y Seguridad de Proveedores Críticos**, el área de compras deberá notificarlo al equipo de SGI. Esta notificación debe estar acompañada de la confirmación de aprobación del proveedor.
- d. **Notificación de finalización del servicio:** Cuando un proveedor finalice su relación contractual con REDFACILITO, el responsable del área correspondiente deberá notificarlo al equipo de SGI y al área legal para proceder con la baja del riesgo asociado a dicho proveedor en la matriz correspondiente.
- e. **Revisión anual de riesgos de proveedores:** Una vez al año, el equipo de SGI revisará, junto con el responsable del área correspondiente, la matriz de riesgos de proveedores para confirmar si los riesgos existentes deben mantenerse o si deben incorporarse nuevos. No obstante, si en cualquier momento se identifica un nuevo riesgo que no fue contemplado en la revisión anual, el responsable del área podrá notificarlo de inmediato al equipo de SGI.
- f. **Control de evaluaciones de seguridad:** El equipo de SGI será responsable de registrar la fecha de evaluación de seguridad de la información de cada proveedor en la matriz de riesgos. Al cumplirse un año desde la última evaluación, deberá solicitarse al proveedor evidencia actualizada del cumplimiento de los controles declarados,

esta gestión de solicitar la hace el líder de área y remite evidencias al equipo del SGI. Este proceso se repetirá anualmente mientras el proveedor permanezca activo. (La responsabilidad de seguimiento por parte del equipo del SGI recae únicamente con el líder de área, el resto de gestión directa con el proveedor lo debe hacer el líder de área)

- g. **Seguimiento de controles declarados:** El seguimiento directo de los controles declarados en la matriz de riesgos corresponde al líder del área que mantiene la relación con el proveedor. Sin embargo, el equipo de SGI será responsable de validar que, dentro del periodo de un año desde la declaración inicial, se haya solicitado al proveedor evidencia actualizada del cumplimiento de dichos controles.

5.8 Usuarios y contraseñas

- a. Los proveedores con acceso a sistemas de información, deberá utilizar credenciales únicas por cada usuario y servicio a utilizar, los proveedores son responsables de las actividades que se realicen con el uso de sus credenciales.
- b. Los proveedores no deben revelar sus credenciales de acceso a otra persona, ni mantenerla por escrito a la vista, ni al alcance de terceros.
- c. Las contraseñas deben cumplir con las consideraciones establecidas en el documento **PS-SGS-PO006 - Política de control de contraseñas.**

5.9 Gestión de vulnerabilidades en servidores y/o aplicaciones

- a. En caso de identificar vulnerabilidades en los servidores y/o aplicaciones proporcionadas y administradas por terceros, el proveedor deberá ejecutar las acciones correspondientes para remediar las vulnerabilidades identificadas de manera planificada con REDFACILITO para evitar el impacto al negocio.
- b. La instalación de software por actualización o parches de seguridad deberán realizarse según la recomendación del fabricante en caso de que aplique.

5.10 Revisión de la provisión de servicios

- a. Al menos una vez al año los responsables monitorearán, revisará y/o auditará la prestación de servicios del proveedor con la finalidad de garantizar que el servicio cumple con los requisitos acordados, incluyendo, pero no limitándose a



los acuerdos de niveles de servicio, acuerdos de confidencialidad y acuerdos de intercambio de información.

- b. El Oficial de Seguridad de la Información gestionará el cumplimiento de la revisión anual, dando prioridad a los proveedores críticos, se utilizará el documento **PS-SGS-FR008 - Evaluación de Cumplimiento y Seguridad de Proveedores Críticos**.
- c. Para asegurar que los proveedores que prestan servicios cuenten con estándares de industria en materia de seguridad, la organización se reserva el derecho de solicitar evidencia de la ejecución de auditorías independientes relacionadas al riesgo tecnológico, control interno, o auditorías de certificación relacionados con dicha materia, los cuales deben ser facilitados de manera confidencial y con el objeto de revisar el alcance del trabajo realizado y el detalle de los resultados obtenidos.

5.11 Gestión de cambios en los servicios de los proveedores

- a. Cuando se requiera realizar cambios en la provisión del servicio, estos deben ser notificados por el proveedor a REDFACILITO para determinar el impacto y la posibilidad de evaluar los riesgos.
- b. Los cambios que se lleven a cabo por el proveedor se deberán realizar siguiendo un procedimiento formal y documentado que garantice que se siguen los pasos apropiados para ejecutar el cambio.
- c. Los responsables de área que tengan proveedores críticos en seguridad de la información deberán verificar los cambios en componentes críticos, para comprobar que no se producen efectos adversos o no previstos sobre el funcionamiento o la seguridad de dichos componentes.

5.12 Seguridad en el desarrollo de software

- a. Los proveedores que realicen actividades de desarrollo de software serán controlados y supervisados por los Analista Senior de Desarrollo y los proveedores deberán asegurar el cumplimiento de los lineamientos del documento **PS-SGS-PO009 - Política de desarrollo seguro**.
- b. Las especificaciones de los aplicativos deberán contener expresamente los requisitos de seguridad a cubrir en cada caso, de acuerdo al documento **TE-DES-DI005 - Requisitos de seguridad técnicos y funcionales en los desarrollos**.



5.13 Transferencia de información con proveedores

- a. Cuando se requiera compartir información con proveedores, para el desarrollo de las actividades contratadas, se deberá realizar mediante las plataformas autorizadas en la organización y los lineamientos establecidos en los documentos **PS-SGS-PO003 - Política de clasificación de la información y medidas de seguridad**, en función de los riesgos que se pudieran identificar y la clasificación de la información a compartir por REDFACILITO puede implementar controles adicionales para la protección de la información.

5.14 Responsabilidades de proveedores y terceras partes con el sistema de gestión de la seguridad de la información

- a. Cumplir con las Políticas de Seguridad de la información de REDFACILITO.
- b. Reportar cualquier incidente de seguridad suscitado en la empresa o que atente a la seguridad de la misma al correo incidentesseguridad@facilito.com.ec.
- c. Apoyar proactivamente a conservar la disponibilidad, integridad y confidencialidad de todo recurso o sistema de información de REDFACILITO.
- d. Firmar y dar cumplimiento al acuerdo de confidencialidad de la información con REDFACILITO.
- e. Aplicar los lineamientos descritos en el documento **PS-SGS-PO006 - Política de control de contraseñas**.
- f. Velar por la protección de los equipos que REDFACILITO que haya puesto a su disposición para el desarrollo de las actividades contratadas.
- g. Proteger la información perteneciente o compartida por REDFACILITO de toda pérdida de confidencialidad, modificación, destrucción o uso inadecuado.

6. DOCUMENTOS RELACIONADOS

Tipo de documento	Código	Nombre
Procedimiento	CN-GCN-PD002	Gestión con proveedores.
Formatos	TE-INF-FR015	Control de acceso lógico a servidores.
Política	PS-SGS-PO005	Política de control de acceso.



Formato	PS-SGS-FR009	Matriz de riesgos de seguridad de la información con proveedores.
Política	PS-SGS-PO006	Política de control de contraseñas.
Formato	PS-SGS-FR008	Evaluación de Cumplimiento y Seguridad de Proveedores Críticos
Política	PS-SGS-PO009	Política de desarrollo seguro.
Documento de Interés	TE-DES-DI005	Requisitos de seguridad técnicos y funcionales en los desarrollos.
Política	PS-SGS-PO003	Política de clasificación de la información y medidas de seguridad.
Política	PS-SGS-PO006	Política de control de contraseñas.

7. LISTA DE DISTRIBUCIÓN

Líder Comercial, Gerente TI, Coordinador de Infraestructura y Ciberseguridad, Líder de Base de datos y producción, Líder de Procesos y SGI, Jefe Legal, Asistente Legal, Analista de Recursos Humanos, Trabajador Social, Contador, Tesorería, Asistente de Compras, Gerente General, Lider Robustos e Inhouse.

